Cisco

351-018

CCIE Security v4.0

QUESTION: 120
Which two identifiers are used by a Cisco Easy VPN Server to reference the correct group policy information for connecting a Cisco Easy VPN Client? (Choose two.)

A. IKE ID_KEY_ID
B. OU field in a certificate that is presented by a client
C. XAUTH username
D. hash of the OTP that is sent during XAUTH challenge/response
E. IKE ID_IPV4_ADDR

Answer: A, B

QUESTION: 121
According ISO27001 ISMS, which of the following are mandatory documents? (Choose 4)

A. ISMS Policy
B. Corrective Action Procedure
C. IS Procedures
D. Risk Assessment Reports
E. Complete Inventory of all information assets

Answer: A, B, C, D

QUESTION: 122
Which current RFC made RFCs 2409, 2407, and 2408 obsolete?

A. RFC 4306
B. RFC 2401
C. RFC 5996
D. RFC 4301
E. RFC 1825

Answer: C

QUESTION: 123
During a computer security forensic investigation, a laptop computer is retrieved that requires content analysis and information retrieval. Which file system is on it, assuming it has the default installation of Microsoft Windows Vista operating system?

A. HSFS
B. WinFS
C. NTFS
D. FAT
E. FAT32

Answer: C

QUESTION: 124
Which of these is a core function of the risk assessment process? (Choose one.)

A. performing regular network upgrades
B. performing network optimization
C. performing network posture validation
D. establishing network baselines
E. prioritizing network roll-outs

Answer: C

QUESTION: 125
Which two answers describe provisions of the SOX Act and its international counterpart Acts? (Choose two.)

A. confidentiality and integrity of customer records and credit card information
B. accountability in the event of corporate fraud
C. financial information handled by entities such as banks, and mortgage and insurance brokers
D. assurance of the accuracy of financial records
E. US Federal government information
F. security standards that protect healthcare patient data

Answer: B, D

QUESTION: 126
Which three statements about the IANA are true? (Choose three.)

A. IANA is a department that is operated by the IETF.

B. IANA oversees global IP address allocation.
C. IANA managed the root zone in the DNS.
D. IANA is administered by the ICANN.
E. IANA defines URI schemes for use on the Internet.

Answer: B, C, D

QUESTION: 127
What does the Common Criteria (CC) standard define?

A. The current list of Common Vulnerabilities and Exposures (CVEs)
B. The U.S standards for encryption export regulations
C. Tools to support the development of pivotal, forward-looking information system technologies
D. The international standards for evaluating trust in information systems and products
E. The international standards for privacy laws
F. The standards for establishing a security incident response system

Answer: D

QUESTION: 128
Which three types of information could be used during the incident response investigation phase? (Choose three.)

A. netflow data
B. SNMP alerts
C. encryption policy
D. syslog output
E. IT compliance reports

Answer: A, B, D

QUESTION: 129
Which of the following best describes Chain of Evidence in the context of security forensics?

A. Evidence is locked down, but not necessarily authenticated.
B. Evidence is controlled and accounted for to maintain its authenticity and integrity.
C. The general whereabouts of evidence is known.

D. Someone knows where the evidence is and can say who had it if it is not logged.

Answer: B

QUESTION: 130
Which option is a benefit of implementing RFC 2827?

A. prevents DoS from legitimate, non-hostile end systems
B. prevents disruption of special services such as Mobile IP
C. defeats DoS attacks which employ IP source address spoofing
D. restricts directed broadcasts at the ingress router
E. allows DHCP or BOOTP packets to reach the relay agents as appropriate

Answer: C

Pass your exam at First Attempt....Guaranteed!